UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,776	03/22/2004	Gene A. Frantz	TI-37762	9940

23494 7590 08/21/2009

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/21/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com

Office Action Summary	Application No.	Applicant(s)	
	10/805,776	FRANTZ, GENE A.	
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-15,18,19,21 and 23-25* is/are pending in the application.

4a) Of the above claim(s) *7,16,17,20 and 22* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-15,18,19,21 and 23-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-6, 8-15, 18-19, 21, and 23-25 are pending.

Claims 7,16,17,20 and 22 are cancelled.

Response to Arguments

2. Applicant's arguments filed 5/1/2009 have been fully considered but they are not persuasive.

Regarding the argument on pg.7, that Folmsbee does not read, teach, or suggest decrypting software as required by claims 1, 6, 11, and 19. Folmsbee discusses decoding prior to execution where providing correct intermediate result in an instruction decoder that accepts instruction op codes in excess of a set of instruction op codes required for execution of a program (col.3, lines 8-44). Folmsbee discloses while the inventive CPU 11 is designed to receive scrambled instructions but not to decrypt them. Then, discusses the programs themselves can be written in such a way that data decryption is performed and data encryption and decryption software can be written for the inventive CPU 11 (col.7, lines 1-11). Folmsbee discloses the software company decrypts the encrypted key with its private key and (col.19, lines 20-30). Thus, obviously suggests there was prior art at the time of applicant's invention was made that decryption of software program exists to decrypt the encrypted data program. As for the secondary prior art, Srinivasan is combined with Folmsbee that it would have been

obvious for a person of ordinary skills in the art for the processor to access the unique ID because this assures application software and multimedia content are only used on processors when the right to do so has been authorized without having to substantially alter the original application software and reduction in speed or other resources available to the application software (Srinivasan - col.1, lines 43-49 and 63-67 and col.2, lines 23-28). Therefore, Folmsbee and Srinivasan combination reads on the claimed invention.

Regarding the argument on pg.7 for claim 21 and 23-25, that Folmsbee does not read, teach, or suggest decrypting a software file as required by claim 21. As discussed above, Folmsbee discusses decoding prior to execution where providing correct intermediate result in an instruction decoder that accepts instruction op codes in excess of a set of instruction op codes required for execution of a program (col.3, lines 8-44). Folmsbee discloses while the inventive CPU 11 is designed to receive scrambled instructions but not to decrypt them. Then, discusses the programs themselves can be written in such a way that data decryption is performed and data encryption and decryption software can be written for the inventive CPU 11 (col.7, lines 1-11). Folmsbee discloses the software company decrypts the encrypted key with its private key and (col.19, lines 20-30). Thus, obviously suggests there was prior art at the time of applicant's invention was made that decryption of software program exists to decrypt the encrypted data program. Therefore, Folmsbee and Hejna combination reads on the claimed invention for it would have been obvious for a person of ordinary skills in the art to include multiple processors because making use of several processors can execute

concurrently and to speed execution of the processes whereby improving the efficiency of process scheduling in a multiprocessor system (Hejna on col.1, lines 7-10 and col.8, lines 38-45).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 8-15, and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Folmsbee (US 7,225,322), and further in view of Srinivasan, et al. (US 7,380,275).

As per claim 1:

Folmsbee discloses a data processing unit for executing an encrypted software executable program, the data processing unit comprising:

a processor for decrypting the encrypted executable program and for executing the software program (col.7, lines 2-12 and col.8, lines 23-26), the processor including an identifying number functioning as a serial number for identifying the data processing unit (col.14, lines 10-20 and col.19, lines 20-30), the identifying number being accessible only by the processor; and (col.1, lines 58-60 and col.14, lines 10-60)

a memory unit, the memory unit storing the decryption procedure (col.5, lines 29-31 and col.18, lines 42-52), the encrypted executable program being encrypted using at least a portion of the identifying number; (col.8, lines 35-40 and col.22, lines 55-59)

wherein, when the processor is to execute the executable program, the executable program is decrypted using the decryption procedure along with the identifying number. (col.7, lines 1-11 and col.19, lines 20-30)

Folmsbee discloses the CPU (processor) includes serial number and having a plurality of memory stores (col.5, lines 29-31 – i.e. RAM, EPROM, ROM) for storing the serial numbers (col.13, lines 16-36). Folmsbee discusses the program is identified by a key and a serial number of the CPU, stored on the CPU (col.8, lines 37-40) which to provide verification of the authenticity (col.9, lines 35-37). However, Folmsbee did not specify the serial number (identifying number) being accessible only by the processor.

Srinivasan, et al. teaches a secure processor assuring application software is executed securely and assuring only authorized software is executed (abstract). The secure processor maintains security information (col.11, lines 55-59) such as the unique ID, code signatures or cryptographic hashes, and unique encryption/decryption keys as well as other information to the particular processor (col.4, lines 19-14). Srinivasan discloses the CPU memory interface receives memory access requests from the CPU and performs appropriated interface functions with the external memory (col.9, lines 45-62). Further, the CPU is allowed to access the secure boot code, execute its instructions, and read/write data using the security information (col.13, lines 13-16). Whereby the CPU executes software and that the decryption keys from the read-only

secure data accessible only by the CPU while in secure mode (col.13, lines 55-62). Thus, suggests only the authorized CPU is able to access security information (unique ID).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the processor to access the unique ID of Srinivasan with the processor having the serial number of Folmsbee because this assures application software and multimedia content are only used on processors when the right to do so has been authorized without having to substantially alter the original application software and reduction in speed or other resources available to the application software (Srinivasan - col.1, lines 43-49 and 63-67 and col.2, lines 23-28).

As per claim 2: see Folmsbee on col.5, lines 20-26; discussing data processing unit as recited in claim wherein the encrypted executable program is stored in the memory unit.

As per claim 3: see Folmsbee on col.15, lines 20-67 and Srinivasan on col.3, lines 55-62; discussing the data processing unit as recited in claim 1 further comprising an external memory unit, wherein the encrypted executable program is stored in an external memory unit.

As per claim 4: see Folmsbee on col.4, lines 47-48; discussing the data processing unit as recited in claim 1 wherein the identifying number is a serial number.

As per claim 5: see Folmsbee on col.4, lines 46-65 and col.8, lines 36-40; discussing the data processing unit as recited in claim 1 wherein the identifying number is associated with a plurality of data processing units.

As per claim 6:

Folmsbee discloses a method for protecting software programs, the method comprising:

providing a data processing unit with an identifying number (col.14, lines 10-20 and col.19, lines 20-30), the identifying number being accessible only by the processing unit functioning as a serial number for identifying the data processing unit; (col.4, lines 45-54 and col.10, lines 35-40)

encrypting a executable program external to the data processing unit (col.15, lines 20-67) using at least a portion of the identifying number; and (col.8, lines 35-40 and col.18, lines 42-52)

decrypting the encrypted executable program (col.7, lines 1-11 and col.19, lines 20-30) prior for execution of the executable program by the data processing unit (col.7, lines 2-12 and col.8, lines 23-26) using the identifying number and a decryption procedure in the processing unit. (col.5, lines 29-31 and col.22, lines 55-59)

Folmsbee discloses the CPU (processor) includes serial number and having a plurality of memory stores (col.5, lines 29-31 – i.e. RAM, EPROM, ROM) for storing the serial numbers (col.13, lines 16-36). Folmsbee discusses the program is identified by a key and a serial number of the CPU, stored on the CPU (col.8, lines 37-40) which to provide verification of the authenticity (col.9, lines 35-37). However, Folmsbee did not specify the serial number (identifying number) being accessible only by the processor.

Srinivasan, et al. teaches a secure processor assuring application software is executed securely and assuring only authorized software is executed (abstract). The

secure processor maintains security information (col.11, lines 55-59) such as the unique ID, code signatures or cryptographic hashes, and unique encryption/decryption keys as well as other information to the particular processor (col.4, lines 19-14). Srinivasan discloses the CPU memory interface receives memory access requests from the CPU and performs appropriated interface functions with the external memory (col.9, lines 45-62). Further, the CPU is allowed to access the secure boot code, execute its instructions, and read/write data using the security information (col.13, lines 13-16). Whereby the CPU executes software and that the decryption keys from the read-only secure data accessible only by the CPU while in secure mode (col.13, lines 55-62). Thus, suggests only the authorized CPU is able to access security information (unique ID).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the processor to access the unique ID of Srinivasan with the processor having the serial number of Folmsbee because this assures application software and multimedia content are only used on processors when the right to do so has been authorized without having to substantially alter the original application software and reduction in speed or other resources available to the application software (Srinivasan - col.1, lines 43-49 and 63-67 and col.2, lines 23-28).

As per claim 7: Cancelled

As per claim 8: see Folmsbee on col.4, lines 47-48; discussing the method as recited in claim 6 wherein the identifying number is a serial number for the data processing unit.

As per claim 9: see Folmsbee on col.15, lines 20-67 and Srinivasan on col.3, lines 55-62; discussing the method as recited in claim 6 wherein the encrypted executable program is stored external to the data processing unit.

As per claim 10: see Folmsbee on col.4, lines 46-65 and col.8, lines 36-40; discussing the method as recited in claim 6 wherein the encrypted executable program is stored in data processing unit.

As per claim 11:

Folmsbee discloses a data processing system, the system comprising:

a host data processing unit the host processing unit encrypting executable program using at least a portion of an identifying number functioning as a serial number (col.14, lines 10-20 and col.19, lines 20-30) for identifying the data processing unit; and (col.8, lines 35-40 and col.18, lines 42-52)

a target data processing unit, the target data processing unit decrypting executable program (col.7, lines 1-11 and col.19, lines 20-30) with a software procedure using a decryption key based on the identifying number. (col.5, lines 7-31 and col.9, lines 30-49 and col.22, lines 55-59)

Folmsbee discloses the CPU (processor) includes serial number and having a plurality of memory stores (col.5, lines 29-31 – i.e. RAM, EPROM, ROM) for storing the serial numbers (col.13, lines 16-36). Folmsbee discusses the program is identified by a key and a serial number of the CPU, stored on the CPU (col.8, lines 37-40) which to provide verification of the authenticity (col.9, lines 35-37). However, Folmsbee did not specify the serial number (identifying number) being accessible only by the processor.

Srinivasan, et al. teaches a secure processor assuring application software is executed securely and assuring only authorized software is executed (abstract). The secure processor maintains security information (col.11, lines 55-59) such as the unique ID, code signatures or cryptographic hashes, and unique encryption/decryption keys as well as other information to the particular processor (col.4, lines 19-14). Srinivasan discloses the CPU memory interface receives memory access requests from the CPU and performs appropriated interface functions with the external memory (col.9, lines 45-62). Further, the CPU is allowed to access the secure boot code, execute its instructions, and read/write data using the security information (col.13, lines 13-16). Whereby the CPU executes software and that the decryption keys from the read-only secure data accessible only by the CPU while in secure mode (col.13, lines 55-62). Thus, suggests only the authorized CPU is able to access security information (unique ID).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the processor to access the unique ID of Srinivasan with the processor having the serial number of Folmsbee because this assures application software and multimedia content are only used on processors when the right to do so has been authorized without having to substantially alter the original application software and reduction in speed or other resources available to the application software (Srinivasan - col.1, lines 43-49 and 63-67 and col.2, lines 23-28).

As per claim 12: see Folmsbee on col.4, lines 47-48; discussing the system as recited in claim 11 wherein the identifying number is a serial number for the target data process

As per claim 13: Folmsbee on col.15, lines 20-67 and Srinivasan on col.3, lines 55-62; discussing the system as recited in claim 11 further comprising a memory unit external to the target data processing unit, the memory unit storing encrypted executable program unit.

As per claim 14: see Folmsbee on col.5, lines 20-26 and col.10, lines 5-29; discussing the system as recited in claim 11 further comprising a memory unit in the target data processing unit, the memory unit storing encrypted executable programs prior to decryption.

As per claim 15: see Folmsbee on col.7, lines 8-11 and col.19, lines 21-40; discussing the system as recited in claim 11 wherein an encrypted program is decrypted as an entity or on the fly prior to execution of the executable program by the target data processing unit.

As per claims 16-17: Cancelled.

As per claim 18: see Folmsbee on col.5, lines 20-26 and col.10, lines 5-29; discussing the system as recited in claim 15 wherein decrypted portions of the executable program are stored in a protected memory unit accessible to only the target data processing unit.

As per claim 19:

Folmsbee discloses a method for protecting an execution of an executable file, the method comprising:

providing a target processor with an identifying number, functioning as a serial number for identifying the data processing unit, accessible only to the target processor; (col.14, lines 10-20 and col.19, lines 20-30)

encrypting the executable file using at least a portion of the identifying/serial number; (col.8, lines 35-40 and col.18, lines 42-52)

applying the encrypted executable file to the target processor; (col.7, lines 2-12 and col.8, lines 23-26)

decrypting the encrypted executable file using a decryption procedure stored in the target processor and the identifying/serial number. (col.7, lines 1-11 and col.19, lines 20-30)

Folmsbee discloses the CPU (processor) includes serial number and having a plurality of memory stores (col.5, lines 29-31 – i.e. RAM, EPROM, ROM) for storing the serial numbers (col.13, lines 16-36). Folmsbee discusses the program is identified by a key and a serial number of the CPU, stored on the CPU (col.8, lines 37-40) which to provide verification of the authenticity (col.9, lines 35-37). However, Folmsbee did not specify the serial number (identifying number) being accessible only by the processor.

Srinivasan, et al. teaches a secure processor assuring application software is executed securely and assuring only authorized software is executed (abstract). The secure processor maintains security information (col.11, lines 55-59) such as the unique ID, code signatures or cryptographic hashes, and unique encryption/decryption keys as well as other information to the particular processor (col.4, lines 19-14). Srinivasan discloses the CPU memory interface receives memory access requests from the CPU and performs appropriated interface functions with the external memory (col.9, lines 45-62). Further, the CPU is allowed to access the secure boot code, execute its instructions, and read/write data using the security information (col.13, lines 13-16).

Whereby the CPU executes software and that the decryption keys from the read-only secure data accessible only by the CPU while in secure mode (col.13, lines 55-62). Thus, suggests only the authorized CPU is able to access security information (unique ID).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the processor to access the unique ID of Srinivasan with the processor having the serial number of Folmsbee because this assures application software and multimedia content are only used on processors when the right to do so has been authorized without having to substantially alter the original application software and reduction in speed or other resources available to the application software (Srinivasan - col.1, lines 43-49 and 63-67 and col.2, lines 23-28).

As per claim 20: Cancelled.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 21 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Folmsbee (US 7,225,322), and further in view of Hejna, et al. (US 5,287,508).

As per claim 21:

Folmsbee discloses an apparatus for secure transfer of software files, the apparatus comprising:

a first processor, the first processor having program for encrypting an executable file (col.8, lines 35-40 and col.18, lines 42-52) using an identifying number, functioning as a serial number for identifying the data processing unit; and (col.1, lines 58-60 and col.14, lines 10-60)

a second processor, the second processor having a decryption procedure stored in a memory coupled to the second processor for decrypting the executable file using at least a portion of the identifying/serial number stored in the second processor, the stored identifying/serial number being accessible only to the second processor; (col.7, lines 1-11 and col.19, lines 20-30)

Folmsbee suggests each CPU could be provided with different key (col.10, lines 45-54) which is individual keys for individual CPUs (col.22, lines 50-61) identified by serial numbers (col.1, lines 58-62) and wherein the first processor encrypts the software file using a copy of the at least a portion of the identifying/serial number. (col.8, lines 35-40 and col.22, lines 55-59). However, Folmsbee did not clearly discuss multiple processors such as the claimed first processor and a second processor.

Hejna, et al. discloses improving the efficiency of process scheduling in a multiprocessor system by including plurality of processors and schedules processes according to the priority of the process (col.1, lines 7-10 and col.2, lines 50-67). Hejna discloses a multiprocessor system in which memory is shared by all processors can

execute different process concurrently or can execute different threads (from one or multiple processes) concurrently (col.7, line 67 – col.8, line 16). Thus, make use of several processors to speed execution of the processes (col.8, lines 38-45).

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of Folmsbee with Hejna teaching multiple processors because making use of several processors can execute concurrently and to speed execution of the processes whereby improving the efficiency of process scheduling in a multiprocessor system (Hejna on col.1, lines 7-10 and col.8, lines 38-45).

As per claim 22: Cancelled

As per claim 23: see Folmsbee on col.4, lines 62-67 and col.9, lines 35-48; discussing the apparatus as recited in claim 21 wherein the at least a portion of the identifying/serial number is accessed by the first processor based on an indicia of the second processor.

As per claim 24: see Folmsbee on col.7, lines 8-11; discussing the apparatus as recited in claim 21 wherein an encrypted executable file is stored in an unsecured storage unit.

As per claim 25: see Folmsbee on col.19, lines 21-40 and col.22, lines 55-59; discussing the apparatus as recited in claim 24 wherein the encrypted executable file is stored in the unsecured storage unit prior to decryption.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435